

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
20 janvier 2005 (20.01.2005)

PCT

(10) Numéro de publication internationale  
**WO 2005/006706 A1**

(51) Classification internationale des brevets<sup>7</sup> : **H04L 29/06**

(72) Inventeur; et

(21) Numéro de la demande internationale :

PCT/IB2004/051130

(75) Inventeur/Déposant (pour US seulement) : **MOREIL-  
LON, Guy** [CH/CH]; Rue Saint-Denis 4, CH-1040 Échal-  
lens (CH).

(22) Date de dépôt international : 6 juillet 2004 (06.07.2004)

(74) Mandataire : **LEMAN CONSULTING SA**; Route de  
Clémenty 62, CH-1260 Nyon (CH).

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

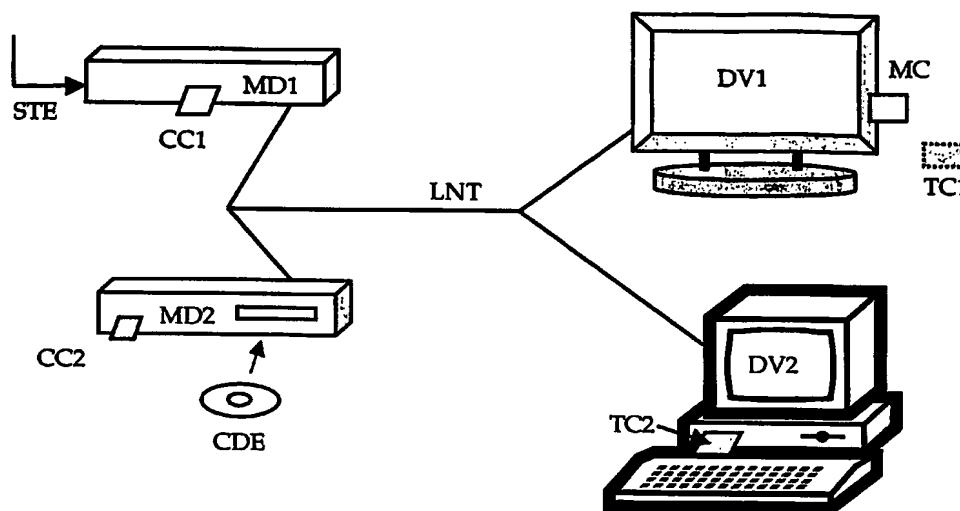
01233/03 14 juillet 2003 (14.07.2003) CH

(81) États désignés (sauf indication contraire, pour tout titre de  
protection nationale disponible) : AE, AG, AL, AM, AT,  
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,  
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,  
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,  
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,  
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,  
PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN,  
TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD FOR GENERATING AND MANAGING A LOCAL AREA NETWORK

(54) Titre : MÉTHODE DE CRÉATION ET D'ADMINISTRATION D'UN RÉSEAU LOCAL



(57) Abstract: The invention relates to a method for generating and managing a local area network including at least one device for reproducing an encrypted data flow and a device for transmitting and re-encrypting all or part of said encrypted data, which devices include security modules. The method includes the steps of connecting a so-called master security module in one of the devices connected to the local area network, causing the master security module to generate a network key, securely transmitting the network key to one or more so-called user security modules, decrypting the data encrypted by the transmission and re-encryption device, re-encrypting the data with said device by means of a local key, transmitting the re-encrypted data to the reproduction device, and holding the reproduction device to perform decryption using the user security module associated therewith and provided with means for locating the local key.

[Suite sur la page suivante]

WO 2005/006706 A1

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SI., SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

**Publiée :**

— avec rapport de recherche internationale

(57) **Abstré :** La présente invention propose une méthode de création et d'administration d'un réseau local, ce réseau comprenant au moins un dispositif de restitution d'un flux de données chiffrées et un dispositif de diffusion et de rechiffrement de tout ou partie desdites données chiffrées, ces dispositifs comprenant des modules de sécurité, cette méthode comprenant les étapes suivantes: - connexion d'un module de sécurité dit maître dans l'un des dispositifs connecté au réseau local, - établissement d'une clé de réseau par le module de sécurité maître, - transmission sécurisée de cette clé de réseau à un ou des modules de sécurité dits utilisateur, - déchiffrement des données chiffrées par le dispositif de diffusion et de rechiffrement, - rechiffrement des données par ledit dispositif par une clé locale, - transmission des données rechiffrées au dispositif de restitution, - déchiffrement par ledit dispositif de restitution grâce au module de sécurité utilisateur qui lui est associé disposant de moyens pour retrouver la clé locale.